Towards an ontology about trust and security of information systems: joining technology and human perspectives

Káthia Marçal de Oliveira* — Bako Rajaonah* — Pierre-Emmanuel Arduin** — Inès Saad***

* Laboratoire LAMIH – UMR CNRS 8201
Université de Valenciennes - F-59313 Valenciennes cedex 9
Kathia.oliveira@univ-valenciennes.fr, Bako. Rajaonah @univ-valenciennes.fr

** Université Paris-Dauphine, PSL Research University,
Laboratoire DRM UMR CNRS 7088
pierre-emmanuel.arduin@dauphine.fr

*** Laboratoire MIS
Université Picardie Jules Verne
Amiens Business School
ines.saad@u-picardie.fr

RÉSUMÉ. Sécurité et confiance sont deux concepts largement explorés dans la littérature. Sur la sécurité, la communauté informatique recherche de meilleurs algorithmes, protocoles et techniques pour garantir que les systèmes d’information ne soient pas violés par des tiers. Sur la confiance, la psychologie la définit comme un facteur important lorsque des personnes interagitent entre elles et/ou avec des systèmes informatiques. Nous considérons qu’un système d’information est un ensemble de ressources numériques et humaines organisées pour traiter, distribuer et stocker des informations. Par conséquent, la sécurité d’un système d’information peut être vue non seulement d’un point de vue technologique, mais aussi d’un point de vue humain. Sécurité et confiance sont ainsi interdépendantes et, dans cet article, nous présentons une recherche en cours visant à construire une ontologie formelle pour expliciter les connaissances liées à ces concepts et à leurs relations.

ABSTRACT. Security and trust are two concepts largely explored in literature. On the one hand, security has been studied by Computer Science community looking for better algorithms, protocols, and techniques ensuring that information systems are not violated by third parties. On the other hand, trust has been defined in psychology as an important factor when people interact with each other and/or with computer systems. For us, an information system can be seen as a set of digital and human resources organized to process, share and store information. Therefore, the security of an information system can be seen not only from technological, but also from human points of view. Both security and trust are interrelated. In this paper, we present a work-in-progress developing a formal ontology making explicit the knowledge behind these concepts and their relationships.

KEYWORDS: information system, ontology, security, trust
1. Introduction

With the widespread use of technology in different sectors of society, security of information systems has become essential to ensure their better adoption and usage by final users. This need became still more evident with the use of the Internet and the availability of several systems in the Web requiring confidentiality, integrity and reliability of information (Safa and Solms, 2016). Rather than knowledge, the information system carries information source of knowledge. Only individuals can possess genuine knowledge, resulting from their interpretation of information within a certain context (Tsuchiya, 1993). The individual is a carrier of knowledge and a processor of information. He is a component of the Enterprise’s Information and Knowledge System (Arduin et al., 2015). Such a component may be benevolent as well as malevolent. Individuals are entry-points as well as computers and digital artifacts are. The organization has to be aware of such special feature when considering information systems’ security: human behavior is harder to predict and to manage than digital artifacts processing is. As consequence, we considered that security is closed related to trust, in the sense that the information system (IS) should be trusted by its users.

In this paper we present the first steps of a research that aims to identify which knowledge is behind both concepts (trust and security) and how they are interrelated when dealing with the challenge of developing trustworthiness information systems. Next sections present a basic background in the domain, then our approach and our first results are presented.

2. Background Theories

2.1. Security and Trust: Basic Definitions

The main concepts behind IS security are protection of both information and technology against unauthorized access and/or modification (e.g. Dilhon and Backhouse, 2000; Whitman and Mattord, 2011). The problem is therefore to design secure IS, in other words, to design systems such as their users could expect both information and technology to be preserved from unauthorized access and modification. From the perspective of users, IS security is thus a matter of IS trustworthiness: the user’s perceptions of IS would influence his/her expectations that his/her data could not be accessed and/or modified by a third other than him/her and authorized people of IS.

Trust and security in the field of Computer Science have been studied a lot in the literature, but, as underlined by Gollmann (2006), the word ‘trust’ should be avoided when its meaning is not clear. Trust is a psychological state of expectations and the referent of trust (i.e. who/what is trusted) may be people, technology, interaction between human(s) and technology, institution or organization (see McKnight et al. 2011; Rajaonah et al., 2008); consequently, expectations are related to the referent: the trustor expects that the trustee (or referent) will achieve what is expected (behaviour, action, attitude, performance, protection, etc.). The dimensions of trust

...
are the factors that would influence its level and explain users’ expectations (Castelfranchi and Falcone, 2000).

Our focus on this paper is about security. However, some misunderstandings occur when discussing about security and safety. Firesmith (2005) states that “the essential difference between safety and security is that safety deals with accidental harm, whereas security deals with malicious harm, which is harm resulting from attacks or probes by someone or something (e.g., viruses) playing the role of attacker. [...] Safety incidents are either accidents (harm occurs) or near misses, whereas security incidents are successful attacks (harm occurs), unsuccessful attacks (harm does not occur), and probes (i.e., preparations for attacks)”. However, the frontier may be fuzzy because a system may be vulnerable, which can lead to accidents and/or enable attacks. As consequence, although safety is not our main focus, an ontology may tackle ISs’ safety when their security is threatened by safety issues.

To conclude, it may be hypothesised that trust dimensions overlap with IS trustworthiness. The challenge is thus to characterize the dimensions of both users’ trust and IS trustworthiness within the framework of IS security.

2.2 Ontology: Overview

Ontology is a description of entities and their properties, relationships, and constraints expressed via axioms (Gruninger and Fox, 1995).

Stenzhorn et al. (2007) defined three levels of ontologies:

- the Top ontology or Upper-Level ontology that provides a set of abstract concepts for defining any domain;
- the Core domain ontology that defines, for each domain a set of generic concepts;
- the domain ontology that defines, by specialization, the specific concepts for any domain.

Domain ontologies (Guarino, 1998) express conceptualizations that are specific for a particular domain (e.g., transportation, family organization, risks management). They put constraints on the structure and contents of domain knowledge. For instance, when talking about family, one can say that a child must have at least a parent.

Ontologies may serve to various purposes in the context of knowledge management (Anquetil et al., 2007):

- Reference on a domain - explicit knowledge serves as a reference to which people, looking for detailed information on the domain modeled, may use;
- Classification framework - the concepts explicited in an ontology are a good way to categorize information on the domain modeled. Other relations among the concepts of the ontology help one browsing it and finding an information one is looking for;
Interlingua - tools and/or experts wishing to share information on the
domain modeled may use the ontology as a common base to resolve
differing terminologies.

2.3. Related Work

Several works on ontology about security and trust can be found in literature. We
quote, for instance the propositions of Viljanen (2005), Huang and Fox (2006), and
Fenz and Ekelhart (2009).

Viljanen (2005) analyzed thirteen trust models to identify the main features
about trust. As result they assumed that the union of these features across all models
provides a list of trust input factors. These factors were in turn organized in an
initial ontology. This initial ontology consider only concepts, no axiom was defined.

Huang and Fox (2006) also defined an ontology, but focused on transitivity
issues. They discuss that the use of web application implies the need of trust
between entities (sometimes unfamiliar or unknown) that interacts with each other,
and as a consequence trust needs to be transitive. They proposed, therefore, a formal
ontology that makes explicit the semantics for trust transitivity.

Fenz and Ekelhart (2009) have proposed a large ontology that organizes the
knowledge about information security. Their goal is to support and enhance risk
management approaches. To that end they reuse some known taxonomies in the
domain of security and telecommunication.

All these works deals with the concepts of trust and security separately. We
argue that these concepts are interrelated since we believe that the work in digital
information system aims at providing technology that can be trusted by users.

3. Defining an Ontology about Trust and Security: First steps

3.1. Methodology

There are various methodologies to design an ontology (e.g. Gruninger and Fox,
1995, Lopez et al., 1999). All of them consider basically the following phases: (1)
definition of the ontology purpose, (2) conceptualization, (3) formalization, and (4)
validation.

We have defined our ontology using these phases. The purpose of this ontology
is to support software engineers designing trustworthy information systems in terms
of security. In other words, we aim to make explicit what the software engineers
should take into account while developing an information system considering
security aspects in order to provide trustworthy systems. The conceptualization is
the longest step and requires the definition of the ontology’s scope, definition of its
concepts, relations and constraints, and a description of a glossary for all concepts
and attributes specified. It represents the knowledge modeling itself. This step have
been based on a study of the literature about trust and security. The formalization
consists of expressing the ontology in some language and code in a specific tool.
This ontology will be formalized with OWL, using Protégé. Finally the validation is done by instantiating the ontology with real instances examples. Next section we present our on-going work of the conceptualization phase.

3.2. Scope, scenarios of use and Competency Questions

Our goal for developing an ontology is to support software engineers in the development of trustworthy information systems in terms of assuring the users’ confidence in the use of the system. In other words, the software developer should have an answer for the following question: “What should I consider to provide security in a way that the user trusts the system?”

To address this problem, we should take into account two main perspectives: (1) the human, that can be the user (i.e., the trustor), the attackers (that try to attack the system); the software team (managers and software engineers) that develops the system; and (2) the technology, that means the system itself (the trustee).

Based on these perspectives some scenarios of use of this ontology are:

- Software developers need to know which features are important to take into account while developing a system that provides security to ensure trust for the final users.
- Attackers want to discover which technology advances he should overcome to attack the system.
- Managers need to identify information system’s security weaknesses, meaning that they can seek to improve security in order to obtain a higher users’ trust in the information system.
- Attackers want to identify information system’s security weaknesses, meaning that they can seek to improve trust in order to maintain low security levels.

Based on these scenarios, we defined the following competency questions (requirements of the ontology):

a) How can users recognize the information system is trustworthy?
b) Which technologies may be used to provide security in an IS?
c) What are the factors that impact the users’ trust level?
d) What are the system’s features that impact the trustworthiness of the IS?
e) How trust and security are related to provide trustworthiness IS?
f) What more than technologies may be used to provide security in information systems? (management initiatives, deterrence, prevention, etc.)
g) What type of intrusion an IS may suffer?

We have been working interactively to answer each one of these questions by considering the large knowledge disseminated in the literature in several domains. Our approach consists of using the literature and interviewing some experts in security to identify the concepts of the ontology. A first brainstorming of the questions derived the concepts presented in Figure 2.
4. Conclusion and Future Works

In this paper we present the beginning of our research that aims at the definition of an ontology making explicit the knowledge about trust and security considering technology and human perspectives. This ontology is being developed by considering the relevant literature in the subject and validation with domain experts.

The first results of this research consist in the definition of competency questions that will support the identification of the concept and constraints among these concepts. Our ongoing work aims at answering these competency questions and the formalization of the formal ontology.

Bibliography


